CASCADING ROLES AND RESPONSIBILITIES

The Program establishes direct links to the NIH governance structure to reinforce NIH's priority on sound management at the highest possible policy levels and the development and execution of systems that ensure effective, efficient, and ethical use of NIH resources. The final decision-making body in the NIH governance structure is the Steering Committee, chaired by the NIH Director. The individuals and offices below are primarily responsible for ensuring that systems of internal management controls have been established and are operating effectively in the areas for which they have responsibility.

1. **Steering Committee -** The NIH Steering Committee exercises stewardship over the use of NIH resources and provides oversight to ensure that programs are operating within established standards. As such, the Steering Committee oversees assessments of the adequacy of NIH's system of internal management controls, monitors and supports needed corrective actions, and reinforces a climate of management excellence and integrity. Its responsibilities include the following:
    - Provide policy guidance and general oversight to ensure the successful completion of the yearly FMFIA certification/assurance signed by the NIH Director, and the identification and reporting of any material weaknesses.
    - Approve the NIH-wide list of risk areas, their relative ranking, and the NIH-wide Risk Management Plan.
    - Monitor detailed studies and corrective actions to enhance NIH internal controls and risk management activities.
    - Make recommendations to the NIH Director on all policy, procedure, or resource changes needed to ensure the successful operation of the Risk Management Program.
    - Review IC Risk Management Plans and, where appropriate, request corrective action plans and a reassessment by OMA.

2. OD Deputy Director for Management (DDM) – Responsible for ensuring that systems of internal management controls are in place for centralized NIH-wide administrative and research support processes for which she/he is directly responsible, as well as for decentralized processes for which she/he has oversight responsibility. As the Agency's Chief Financial Officer (CFO), the DDM is also responsible (through the Director, Office of Financial Management) for assessing, documenting, and reporting on the effectiveness of internal management controls over financial systems, as required by OMB Circular A-123.

3. OD Deputy Director for Extramural Research – Responsible for ensuring that systems of internal management controls are in place for centralized NIH-wide extramural research and research support processes for which she/he is directly responsible, as well as for decentralized processes for which she/he has oversight responsibility.

4. OD Deputy Director for Intramural Research – Responsible for ensuring that systems of internal management controls are in place for centralized NIH-wide intramural research and research support processes for which she/he is directly responsible, as well as for decentralized processes for which she/he has oversight responsibility.

5. Chief Information Officer (CIO) – Responsible for ensuring that systems of internal management controls are in place for centralized NIH-wide administrative and research support processes, as well as for decentralized processes for which she/he has oversight responsibility.

6. NIH Deputy Directors/CIO

- Sign assurances on the effectiveness of the Risk Management Program in their area of responsibility, ensure that it is effectively carried out and documented to support signed assurances, and develop necessary corrective action plans and time lines for implementation.
- Ensure adequate resources are devoted to risk management and create an environment supportive of risk management at all levels of the organization, holding all NIH senior officials accountable for effective risk management through performance contracts.
- Examine data and periodic risk management reports for trends and patterns and follow up on any possible problems identified.
- Appoint Risk Management Officers (generally EOs) and Risk Area Managers in the areas for which they have responsibility and hold them accountable for their risk management responsibilities through performance contracts.
- Ensure that information and reporting systems are developed and built into automated systems of management controls that enable managers to monitor programs systematically and that alert managers when corrective actions need to be taken.
- Ensure that planning for any major project or initiative includes an assessment of risks, reasonable steps to prevent or mitigate risks, and monitoring to ensure that steps are implemented and effective.
- Work with OMA to develop the NIH-wide Risk Management Plan and make recommendations to OMA concerning (1) any policy, process, procedure, or resource changes that are needed to enhance the program; (2) appropriate communications and training needed to support the program; and (3) areas to include in the NIH-wide Risk Management Plan for detailed review.
- Assess the effectiveness of management controls over financial systems (DDM as the CFO).

7. OD Office Directors and Functional Deputy Directors

- Ensure that risk management plans for risk areas under their purview are effectively carried out and documented to support assurances signed by IC Directors and NIH Deputy Directors.
- Examine data and periodic risk management reports for adverse trends and patterns and ensure that follow-up action is taken on any problems identified.

- Create an environment supportive of risk management at all levels of the organization and establish standard operating procedures to minimize risks.
- Encourage reporting of potential hazards and acknowledge employees for coming forward with identifiable hazards; hold employees accountable for failing to manage, mitigate, or report risks under their purview.
- Ensure that planning for any major project or initiative includes an assessment of risks, reasonable steps to prevent or mitigate them, and monitoring to ensure that steps are implemented and effective.

8. IC Directors - ICs develop their own Risk Management Plans, identifying individual processes under their purview that have potential for significant risks. A comprehensive list of these processes will be developed and updated on an annual basis. ICs will submit the proposed list of processes and risks to the Steering Committee, which, with OMA's assistance, will make a final decision on the composition of the list. IC Directors' responsibilities include the following:

- Sign assurances of the effectiveness of their IC's risk management program, ensure that their Risk Management Plan is carried out effectively and documented to support signed assurances, and develop necessary corrective action plans and time lines for implementation.
- Examine data and periodic risk management reports for adverse trends and patterns and ensure that appropriate follow-up action is taken on any problems identified.
- Delegate specific risk management responsibilities to Executive Officers (RMOs) and others as appropriate and hold them accountable through performance contracts.
- Ensure adequate resources are devoted to risk management, create an environment supportive of risk management at all levels of the organization, and establish standard operating procedures to minimize risks.
- Ensure that planning for any major project or initiative includes an assessment of risks, reasonable steps to prevent or mitigate risks, and monitoring to ensure that steps are implemented and effective.

9. Scientific Directors

- Support the establishment of management controls and risk management program operations so that the momentum cascades down to all scientific and technical levels.
- Encourage the reporting of potential hazards and reward employees for coming forward with identifiable hazards. Hold employees accountable for failing to manage, mitigate, or report risks under their control.
- Examine data and periodic risk management reports for trends and patterns and work to resolve potential problems as they are identified, alerting IC Directors of trends or patterns that may need higher-level attention.
- Ensure that planning for any major project or initiative includes a thorough assessment of risks, reasonable steps to prevent or mitigate risks, and monitoring to ensure that steps are implemented and effective.

10. Risk Management Officers Committee (RMOC) supports and provides resources to the NIH Steering Committee on policies and procedures related to NIH Risk Management Program activities. The RMOC will provide a forum for sharing ideas and best practices related to the development of IC Risk Management Plans and other IC risk management activities and reviews. The RMOC's responsibility is to help support the NIH Risk Management Program and to ensure that all ICs have sufficient risk management assessments to be able to attest to the adequacy of the yearly assurance process. The RMOC shall provide advice on the NIH risk management assessment policy; provide coordination and oversight; and foster communication and cooperation among the NIH ICs, offices, and employees involved in the development of the NIH Risk Management Program to meet the requirements of OMB Circular A-123. RMOC responsibilities include the following:

- Provide support to the Steering Committee to ensure the successful completion of the yearly FMFIA certification/assurance signed by the NIH Director.
- Provide support to the Steering Committee to ensure the successful completion of NIH/IC studies related to enhancing NIH risk management assessment activities.
- Make recommendations to the Steering Committee related to the identification of NIH-wide list of risk areas and the relative ranking of perceived risk. Identify high-risk areas and monitor the successful completion of corrective actions.
- Make recommendations to the Steering Committee on any policy, process, procedure, communication or training needed to enhance the program.
- Provide general oversight of IC Risk Management Plans and make recommendations to the Committee or ICs as needed.
- Ensure that their IC and OD Risk Management Plan is prepared, carried out, and documented each year to support the IC Directors' and NIH Deputy Directors' assurance statements.
- Direct resources to assure adequate funding to support successful operation of the Risk Management Program.
- Create an environment supportive of risk management. Be an advocate of risk management within each IC and OD office, including adequate funding with an emphasis on effective operations.
- Encourage reporting of potential hazards and acknowledge employees for coming forward with identifiable hazards. Hold employees accountable by setting expectations and following through in their performance ratings if they fail to manage, mitigate, or report risks under their purview.
- Examine data and periodic risk management reports for trends and patterns and work to resolve potential problems as they are identified, alerting IC Directors and OD office heads of trends or patterns that may need higher-level attention.
- Ensure that planning for any major project or initiative includes an assessment of risks, reasonable steps to prevent or mitigate risks, and monitoring to ensure that steps are implemented and effective.
- The RMOC meets regularly (on a schedule coordinated by OMA), addresses and resolves operational issues, related to the NIH-wide Risk Management Program, and identifies and shares best practices that could be useful to individual IC/OD risk management programs or to the NIH-wide program. It identifies and

recommends reviews of cross-cutting vulnerabilities that are not NIH-wide but extend beyond one IC. It designates lead ICs to conduct each review.

11. Risk Area Managers – are appointed by Risk Management Officers. They schedule and conduct NIH-wide risk assessments and management control reviews in their area:

- Assemble related reports, reviews, and best practices, including those from other agencies, for use in risk assessments and management control reviews in their area.
- Identify, select, and lead assessments and the review teams, composed of OD and IC staff.
- Develop a study plan for each management control review and report on any identified weaknesses.
- Develop and implement corrective action plans that include a systemic approach, with indicators of success and information systems to provide early warning of potential problems.
- Schedule and conduct corrective action reviews in coordination with OMA.
- Notify the OMA Director and the DDM of any serious material weaknesses.

OMA: 6011 Executive Blvd., Suite 601; (301) 496-2461

DDM: Building 1, Room 102; (301) 496-3271

12. Supervisors/Managers - All NIH managers are responsible for ensuring that internal management control is an important part of their normal duties. They are also responsible and accountable for ensuring that management systems and performance indicators are in place to measure performance across the full spectrum of processes and administrative areas under their purview and to proactively take corrective action when necessary. This responsibility includes managers of centralized processes and support activities at the OD level as well as IC managers administering IC-specific processes and decentralized processes and support services.

The program's foundation is accountability. The execution of internal management control responsibilities shall be a component of the performance contract of all appropriate NIH employees.

As managers review their systems of internal management controls, including the need for strengthened controls, they should pay specific attention to the need for safeguards over the release of sensitive information, for a reporting capability that provides an early warning system that ensures operational efficiency and effectiveness, and for compliance with applicable laws and regulations. When initiating new processes to support their programs, managers should build in internal management controls and measures to determine whether the most effective and efficient use of resources is achieved, and whether operations are in compliance with applicable laws and regulations. High priority should be given to proactively ensuring that appropriate performance indicators and process control measures are built into the design and the reporting capability of NIH-

wide Enterprise Systems, with assistance from OMA as necessary. Supervisors / managers:

- Ensure that all employees are aware of their responsibilities to identify, prevent, and mitigate risks and, where necessary, report risks to their supervisors.
- Ensure that employees have the knowledge and skills to effectively carry out their risk management responsibilities.
- Encourage reporting of potential hazards and acknowledge employees for coming forward with identifiable hazards; hold employees accountable for failing to manage, mitigate, or report risks under their purview.
- Develop systematic ways of monitoring performance of activities under their responsibility using quantitative data to the extent possible.
- Ensure that planning for any major project or initiative includes an assessment of risks, reasonable steps to prevent or mitigate them, and monitoring to ensure that steps are implemented and effective.
- Identify, mitigate, and manage risks and take corrective action where necessary, alerting superiors where appropriate.

13. Employees

- Carry out their responsibilities in compliance with all applicable laws, regulations, and policies.
- Work toward "zero defects" in their activities, with the goal to "get it right the first time."
- Identify, prevent, and mitigate risk in their everyday work responsibilities.
- Proactively alert their supervisors to possible problems.
- Work with their supervisors and management to implement corrective actions as needed.

14. Office of Management Assessment (OMA) – Prepares the overall NIH Risk Management Plan, with input from the three NIH OD Deputy Directors and the CIO. The DDM presents the Plan to the Steering Committee, which may request that certain elements be reviewed by other work groups before final action. OMA supports the Steering Committee in its risk management oversight role. It provides periodic reports on the status of controls and corrective actions; and assesses and recommends any changes to policies, processes, procedures, or resources needed to ensure effective risk management at NIH. OMA responsibilities include the following:

- Develop and administer the NIH Risk Management Program; identify assessable processes; identify and prioritize NIH-wide risks; develop and implement the annual NIH-wide Risk Management Plan; and provide technical support to RMOs and Risk Area Managers.
- Perform and oversee reviews and follow-up reviews of high-priority risk areas, as necessary; track NIH-wide reportable conditions, deficiencies, and material weaknesses; and ensure that corrective actions are taken.
- Work with NIH Enterprise System managers and RMOs to ensure that reports are developed to identify and monitor risks and make recommendations to the NIH Deputy Directors or the Steering Committee on the electronic systems or areas that should include controls to enhance risk management capabilities.

- Develop an NIH-wide training and communication strategy for risk management, identifying optimal training requirements, staff to be trained, and appropriate scheduling and delivery of training to meet program requirements.
- Identify best practices for use NIH-wide or in ICs and OD.
- Maintain the Policy Manual chapter on risk management.
- Assist the NIH Deputy Directors, the CIO, and IC Directors in administering their risk management programs.
- Provide technical support to RMOs and provide staff support, including coordinating and developing the agenda for regularly scheduled meetings of the RMOC.
- Monitor risk management activities undertaken by the ICs and OD functional offices identified as assessable units, including annual reviews of IC and OD Risk Management Plans, including plans for new management control reviews and corrective actions based on the results of previous management control reviews.

15. The Office of Financial Management (OFM) advises the NIH Director and staff and provides leadership and direction for NIH financial management activities; develops policies and instructions for budget preparation and presentation; administers allocation of funds; and manages a system of fund and budgetary controls. Its responsibilities for complying with the requirements of OMB Circular A-123 (Appendix A - Internal Controls over Financial Reporting), in conjunction with OD offices and ICs, include the following:

- Establish a Senior Assessment Team (SAT) comprised of senior NIH officials to monitor and oversee financial reviews and assessments.
- Develop a change management and communications plan to ensure that all parties are familiar with the assessment process, explaining to affected organizations the scope, design, methodology, and the rational behind the assessment.
- Develop, establish, and track internal control processes, application, and documentation to record and report the results of internal control testing, including a methodology for conducting assessments of individual transactions, business processes, and financial reporting.
- Evaluate and document the five components of internal control including the control environment, risk assessment, control activities, information and communication, and monitoring as established by the Government Accountability Office (GAO) in standards for Internal Control in the Federal Government (GAO/AIMD-00-21.3.1). This includes evaluating controls at the process, transaction, and application level and by identifying and documenting key business processes and significant accounts.
- Assure that NIH properly records its transactions using generally accepted accounting principles, and that it processes and summarizes transactions properly to permit preparation of accurate financial statements and supplemental schedules.
- Identify, document, and assess internal control design for each business process and financial reporting objective to provide reasonable assurance

that financial transactions are recorded accurately in the accounting system and in financial reports.

- Test accounting transactions to determine that controls are designed properly and operate effectively.
- Prepare an assessment report summarizing the assessment methodology, scope, results, and recommendations to address any identified internal control challenges, including an analysis of internal controls over financial reporting that are not consistent with the revised circular.
- Provide Assurance Statement, as defined in OMB Circular A-127, Financial Management Systems, and OMB's Implementation Guidance for the Federal Financial Management Improvement Act (FMFIA) of 1996, that NIH financial systems, as a whole, satisfy most policies and standards prescribed for executive agencies in developing, operating, and reporting on financial management systems.